Amendments to the Claims:

1.   (Previously Presented) A method for sending secure messages in a broadcast network comprising the steps of:

encrypting data with a key;

hashing said key;

combining said encrypted data and said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of wireless receiving nodes;

wirelessly transmitting said broadcast message to the plurality of wireless receiving nodes; and

removing at least one node from the plurality of wireless receiving nodes by transmitting a message including a NULL key to the node to be removed with the message configured such that the node to be removed replaces said key with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key.

2.   (Previously presented) The method of claim 1 wherein the key is one of a plurality of different keys and said steps of combining and transmitting comprises:

combining said encrypted data with each one of said plurality of different keys in a plurality of broadcast messages; and

transmitting one of the plurality of broadcast messages to a subset of said plurality of receiving nodes.

3.   (Previously presented) The method of claim 2 wherein each one of said plurality of different keys is associated with a respective category of messages.

4.   (Currently Amended) A method for decrypting a message received over a broadcast network comprising the steps of:

receiving data comprising an encrypted message and a hashed key at a node in said broadcast network, wherein said node comprises means for storing data;

parsing said data to derive said encrypted message and said hashed key;

comparing said received hashed key with a plurality of keys that are prestored in said means for storing data in said node and to select a key having a hash matching said received hashed key; ~~and~~

decrypting said encrypted message with said matching key if a match was found; and

requesting a key from a network entity if no prestored key is found to have a hash that matches said received hashed key.

5. (Cancelled)

6. (Previously Presented) In a communications network having a plurality of network entities, a first one of the network entities comprising:

a means encrypting data with a key;

a means for hashing said key;

a means for combining said encrypted data and said key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of wireless receiving nodes;

a means for wirelessly transmitting said broadcast message to the plurality of wireless receiving nodes; and

a means for removing at least one node from the plurality of wireless receiving nodes by transmitting a message including a NULL key to the node to be removed with the message configured such that the node to be removed replaces said key with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key.

7. (Currently Amended) The network entity of claim [[5]] 4 further comprising a means for distributing hashed keys.

8. (Currently amended) A computer-readable memory having computer-readable program code portions stored therein for directing a computer to function in a particular manner when used by the computer, the computer-readable program code portions comprising:

a first portion to direct the computer to encrypt data with a key;

a second portion to direct computer to hash said key;

a third portion to direct computer to combine said encrypted data with said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of wireless receiving nodes;

a fourth portion to direct computer to provide multiple wireless transmissions of said message; and

a fifth portion to direct the computer to remove at least one node from the plurality of wireless receiving nodes by transmitting a message including a NULL key to the node to be removed with the message configured such that the node to be removed replaces said key with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key.

9.   (Currently Amended) A computer-readable memory <u>having computer-readable program code portions stored therein</u> for directing a computer to function in a particular manner when used by the computer, <u>the computer-readable program code portions</u> comprising:

a first portion to direct the computer to receive data comprising an encrypted message and a hashed key;

a second portion to direct computer to parse said data;

a third portion to direct computer to compare said received hashed key with a plurality of keys and to select a key having a hash matching said received hashed key; and

a fourth portion to direct computer to decrypt said encrypted message with said matching key if a match was found and send request for key to a network entity if no matching key was found.

10.   (Currently Amended) A computer <u>program product comprising at least one computer-readable storage medium having computer-readable program code portions stored therein, the computer-readable program code portions comprising</u> ~~data signal embodied in a carrier wave, comprising an encrypted message, a hashed key~~ <u>and</u> ~~instructions for~~:

<u>a first executable portion for</u> parsing <u>received data comprising an encrypted message and a hashed key</u> ~~said data~~ to derive said encrypted message and said hashed key;

4

a second executable portion for comparing said received hashed key with a plurality of keys that are prestored by a receiving node to select a key having a hash matching said received hashed key; and

a third executable portion for decrypting said encrypted message with said matching key if a match was found and sending request for key to a network entity if no matching key was found.

11.   (Previously Presented) A computer program product that enables a network entity to distribute secure content in a network comprising:

computer readable code that instructs computer to:

encrypt data with a key;

hash said key;

combine said encrypted data and said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of wireless receiving nodes;

wirelessly transmit multiple transmissions of said broadcast message; and

remove at least one node from the plurality of wireless receiving nodes by transmitting a message including a NULL key to the node to be removed with the message configured such that the node to be removed replaces said key with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key

and

a tangible medium that stores the computer readable code.

12.   (Original) The computer product of claim 11 wherein the tangible medium is selected from a group consisting of hard-disk, CD-ROM, DVD, floppy disk, flash memory and the like.

13.   (Previously Presented) A computer-readable memory of claim 9 wherein said third portion is adapted to compare said received hashed key with a plurality of keys that have been prestored by the computer.

14.   (Currently Amended) A method of claim 4 wherein receiving data comprises receiving the same data comprising an encrypted message and a hashed key at each of a plurality of nodes in said broadcast network, and wherein said parsing, comparing and decrypting ~~steps~~ are performed at each of the plurality of nodes in said broadcast network.

Claims 15-18   (Canceled).